Algebra

Larry C. Grove

Algebra

Larry C. Grove

Department of Mathematics
The University of Arizona
Tucson, Arizona

1983

ACADEMIC PRESS
A Subsidiary of Harcourt Brace Jovanovich, Publishers

New York London
Paris San Diego San Francisco São Paulo Sydney Tokyo Toronto

ACADEMIC PRESS, INC.
111 Fifth Avenue, New York, New York 10003

United Kingdom Edition published by
ACADEMIC PRESS, INC. (LONDON) LTD.
24/28 Oval Road, London NW1 7DX

Library of Congress Cataloging in Publication Data

Grove, Larry C.
Algebra.

(Pure and applied mathematics ;)
Includes index.
1. Algebra, Abstract. I. Title. II. Series: Pure and applied mathematics (Academic Press) ;
QA3.P8 [QA162] 510s [512] 83 2745
ISBN 0 12 304620 3

PRINTED IN THE UNITED STATES OF AMERICA

83 84 85 86 9 8 7 6 5 4 3 2 1

Preface

It is fairly standard at present for first-year graduate students in mathematics in the United States to take a course in abstract algebra. Most, but not all, of them have previously taken an undergraduate algebra course, but the content and substance of that course vary widely. Thus the first graduate course usually begins from first principles but proceeds at a faster pace.

This book is intended as a textbook for that first graduate course. It is based on several years of classroom experience. Any claim to novelty must be on pedagogical grounds. I have attempted to find and use presentations and proofs that are accessible to students, and to provide a reasonable number of concrete examples, which seem to me necessary in order to breathe life into abstract concepts.

My own practice in teaching has been to treat the material in Chapters I–V as the basic course, and to include material from Chapter VI as time permits. There are in Chapters I–V, however, several sections that can be omitted with little consequence for later chapters; examples include the sections on generators and relations, on norms and traces, and on tensor products. The selection of "further topics" in Chapter VI is naturally somewhat arbitrary. Everyone, myself included, will find unfortunate omissions, and *further* further topics will no doubt be inserted by many who use the book. The topics in Chapter VI are more or less independent of one another, but they tend to draw freely on the first five chapters.

There are two types of exercises. Some are sprinkled throughout the text; these are usually straightforward and are intended to clarify the

concepts as they appear. The results of those exercises are often assumed in the following textual material. The other exercises are at the ends of the chapters. They vary widely in difficulty, and are only rarely referred to later. Of course, not all of the exercises are new, and I am indebted to a wide variety of sources.

My debts to earlier textbooks will be clear to those familiar with the sources, but particular mention should be made of the works of Artin [1–4], Van der Waerden [37], Jacobson [17], Zariski–Samuel [41], and Curtis–Reiner [8]. I have followed Kaplansky's elegant version of the Fundamental Theorem of Galois theory.

I have learned more than I can reasonably acknowledge from my colleagues, past and present. I hope they know who they are and accept my gratitude. The same applies to a large number of students, who have suffered through several preliminary versions and who have prompted many improvements. I must single out Kwang Shang Wang and Javier Gomez Calderon, who ferreted out large numbers of mistakes, misprints, and obscurities by means of several careful rereadings.

Finally, my best thanks go to Helen for all the typing and all the rest.

List of Symbols

$\leq$	Subgroup of
$\lhd$	Normal subgroup of
$\prod$	Product
$\times$	Cartesian product, direct product
$\oplus$	Direct sum
$\vee$	Join
$\bigotimes_R$	Tensor product over ring R
$\mathbb{A}$	Field of algebraic numbers
$a \mid b$	a is a divisor of b; b is a multiple of a
$a \sim b$	a and b are associates
$[A, B]$	The group generated by commutators $[x, y]$, $x \in A$ and $y \in B$
ACC	Ascending chain condition
A_n	Alternating group on n letters
Aut G	The automorphism group of group G
$\mathbb{C}$	The field of complex numbers
cf(G)	Class functions on group G
$C_G(x)$	Centralizer of element x in group G
C_{ij}	Column operation; add column i to column j
C_{ijr}	Column operation; add r times column i to column j
cl(x)	Conjugacy class containing group element x
$C(M) = C_R(M)$	Centralizer in ring R of module M
DCC	Descending chain condition
deg $f(x)$, deg $f(X)$	Degree of polynomial
deg T	Degree of representation
D_m	Dihedral group of order $2m$
E_{ij}	Matrix unit, ij-entry is 1 and others are 0
End(A)	Endomorphism ring of abelian group A
$F(a)$	Simple field extension with primitive element a
FHT	Fundamental homomorphism theorem (for groups)
FHTM	Fundamental homomorphism theorem (for modules)

FHTR	Fundamental homomorphism theorem (for rings)
$\mathcal{F}H$	Fixed field of subgroup H
F_q	Galois field with q elements
F_R	Field of fractions of integral domain R
$F(S)$	Extension field of F generated by set S
$f'(x)$	Derivative of polynomial $f(x)$
ϕ_∞	Absolute value function on $\mathbb{C}$
ϕ_p	p-adic valuation on $\mathbb{Q}$
G'	Derived group (commutator subgroup) of group G
GCD	Greatest common divisor
G_f	Galois group of polynomial $f(x)$
$GF(q)$	Galois field with q elements
$G^{(k)}$	Subgroup in the derived series of group G
$G(K:F)$	Galois group of field K over subfield F
$\mathcal{G}L$	Subgroup of Galois group fixing elements of intermediate field L
$GL(n, F)$, $GL(n, q)$, $GL(V)$	General linear group
$\mathbb{H}$	Hamilton's ring of quaternions
$\mathrm{Hom}_R(M, N)$	R-homomorphisms from module M to module N
$\sqrt{I}$	Radical of ideal I
$I(G)$	Inner automorphism group of group G
$\mathrm{Im}(f)$	Image of mapping f
$\mathrm{Int}_S(R)$	Integral closure of subring R in ring S
$(I:R)$	Quotient of ideal I in ring R
$\mathrm{Irr}(G)$	Set of irreducible characters of group G
$J(R)$	Jacobson radical of ring R
$\ker f$	Kernel of homomorphism f
$\ker \chi$	Kernel of character χ
LCM	Least common multiple
$L_k(G)$	Subgroup in descending central series of group G
$m_a(x) = m_{a,F}(x)$	Minimal polynomial over field F of algebraic element a
$M_n(R)$	$n \times n$ matrices over ring R
$M[r]$	Submodule of M annihilated by ring element r
$N = N_{K/F}$	Norm function from field K to subfield F
$N_G(A)$	Normalizer in group G of subset A
$\mathrm{Orb}_G(s)$	Orbit of element s under action of group G
$\mathrm{Perm}(S)$	Group of permutations of set S
PID	Principal ideal domain
$\mathrm{PSL}(n, F)$, $\mathrm{PSL}(n, q)$, $\mathrm{PSL}(V)$	Projective special linear group
$\mathbb{Q}$	Field of rational numbers
Q_2	Quaternion group, order 8
Q_m	Generalized quaternion group, order $4m$
$\mathbb{R}$	Field of real numbers
R^*	Nonzero elements in ring R
RG	Group algebra of group G over commutative ring R
R_{ij}	Row operation; add row i to row j
R_{ijr}	Row operation; add r times row i to row j
R_m	Ring of algebraic integers in quadratic field $\mathbb{Q}(\sqrt{m})$

$R\langle S\rangle$	R-module generated by set S
$R[x]$	Ring of polynomials over ring R in indeterminate x
$R(x)$	Field of rational functions over integral domain R in indeterminate x
$R[x_1,\ldots,x_n]$ $= R[X]$	Ring of polynomials over ring R in indeterminates $x_1,\ldots,x_n$
$R(x_1,\ldots,x_n)$ $= R(X)$	Field of rational functions over integral domain R in indeterminates $x_1,\ldots,x_n$
(S)	Ideal generated by subset S of a ring
$\langle S\rangle$	Subgroup generated by subset S of a group
(s)	Principal ideal generated by ring element s
$\mathrm{SL}(n,F)$, $\mathrm{SL}(n,q)$, $\mathrm{SL}(V)$	Special linear group
S_n	Symmetric group on n letters
$\langle S \mid R\rangle$	Group with generating set S subject to set R of relations
$\mathrm{Stab}_G(s)$	Stabilizer of element s under action of group G
$\sigma_i = \sigma_i(x_1,\ldots,x_n)$	ith symmetric polynomial in indeterminates $x_1,\ldots,x_n$
$\mathrm{TD}(K:F)$	Transcendence degree of field K over subfield F
$\mathrm{Tr} = \mathrm{Tr}_{K\,F}$	Trace function from field K to subfield F
UFD	Unique factorization domain
$U(R)$	Group of units in ring R with 1
$V_a(f)$	Variation of a sequence of polynomials at element a of an ordered field
V_T	Module over polynomial ring determined by linear transformation T of vector space V
$\lvert x\rvert$	Order of group element x
$[x,y]$	Commutator of group elements x and y
$\mathbb{Z}$	Ring of integers
$\mathcal{Y} = \mathcal{Y}_{G,S}$	Cycle index of permutation group G on set S
$Z(G)$	Center of group G
$Z_i = Z_i(G)$	Subgroup in ascending central series of group G
$\mathbb{Z}_n$	Ring of integers mod n
$\mathbb{Z}_{p^\infty}$	Divisible abelian p-group; p-primary component of $\mathbb{Q}/\mathbb{Z}$

Introduction

The conventions and notation of elementary set theory are assumed to be familiar to the reader. If $\{S_\alpha : \alpha \in A\}$ is any family of sets, indexed by a set A, we shall write $\prod\{S_\alpha : \alpha \in A\}$, or simply $\prod_\alpha S_\alpha$, for their Cartesian product. Thus $\prod\{S_\alpha : \alpha \in A\}$ is the set of all functions $f: A \to \bigcup\{S_\alpha : \alpha \in A\}$ for which $f(\alpha) \in S_\alpha$, all $\alpha \in A$. If the family $\{S_\alpha\}$ is finite, say $\{S_1, \ldots, S_n\}$, or countable, say $\{S_1, S_2, \ldots\}$, we may write $S_1 \times S_2 \times \cdots \times S_n$, or $S_1 \times S_2 \times \cdots$, respectively, for the Cartesian product. In those cases the elements of the Cartesian product are conveniently represented as ordered n-tuples $(x_1, x_2, \ldots, x_n)$, or sequences $(x_1, x_2, \ldots)$, respectively, where $x_i \in S_i$ for each i. If S and T are sets we write $S \setminus T$ for the relative complement of T in S, i.e., $S \setminus T = \{x \in S : x \notin T\}$.

The cardinality of any set S will be denoted by $|S|$.

A *binary operation* on a set S is a function from the Cartesian product $S \times S$ to the set S. For our purposes a binary operation will often be called *multiplication*, with notation $(x, y) \mapsto xy$, or *addition*, with notation $(x, y) \mapsto x + y$. A binary operation (say multiplication) on a set S is called *associative* if $x(yz) = (xy)z$ for all $x, y, z \in S$.

We shall have occasion to use *Zorn's Lemma*, an equivalent of the set-theoretic *Axiom of Choice*. A brief discussion, with an example of an application, appears in an appendix.

It is assumed that the reader is conversant with the material of a first course in linear algebra, including standard matrix operations and basic facts concerning vector spaces and linear transformations. The existence of a basis and dimension for a vector space are proved in the appendix.

We shall denote the set of integers by $\mathbb{Z}$, the rational numbers by $\mathbb{Q}$, the real numbers by $\mathbb{R}$, and the complex numbers by $\mathbb{C}$. Frequent use will be made of the division algorithm in $\mathbb{Z}$. Also, familiarity with Euler's totient function ϕ will be required on occasion. Details can be found in any book on elementary number theory or in almost any undergraduate abstract algebra book.

Contents

Chapter I | Groups

1. GROUPS, SUBGROUPS, AND HOMOMORPHISMS

A nonempty set with an associative binary operation is called a *semigroup*, and a semigroup S having an *identity element* 1 such that $1x = x1 = x$ for all $x \in S$ is called a *monoid*. Most of the algebraic systems discussed herein will be semigroups or monoids, but almost always with further requirements imposed, so the semigroup or monoid aspect will seldom be explicitly emphasized.

One trivial consequence of the definition of a monoid deserves mention.

Proposition 1.1. The identity element of a monoid S is unique.

Proof. Suppose 1 and e are identities in S. Then $1 = 1e = e$.

A *group* is a set G with an associative binary operation (usually called multiplication) and an identity element 1 satisfying the further requirement that for each $x \in G$ there is an *inverse* element $y \in G$ such that $xy = yx = 1$.

Proposition 1.2. If G is a group and $x \in G$, then x has a unique inverse element.

Proof. Let y and z be inverses for x. Then

$$y = y1 = y(xz) = (yx)z = 1z = z.$$

The unique inverse for $x \in G$ is denoted by x^{-1}. Note that $(x^{-1})^{-1} = x$.

Proposition 1.3. If G is a group and $x, y \in G$, then $(xy)^{-1} = y^{-1}x^{-1}$.

Proof

$$(xy)(y^{-1}x^{-1}) = ((xy)y^{-1})x^{-1} = (x(yy^{-1}))x^{-1} = (x1)x^{-1} = xx^{-1} = 1,$$

and similarly $(y^{-1}x^{-1})(xy) = 1$.

As Coxeter [7] has pointed out, the "reversal of order" in Proposition 1.3 becomes clear when we think of the operations of putting on our shoes and socks.

If the binary operation of a group G is written as addition, then the identity element is commonly denoted by 0 rather than 1, and the inverse of x by $-x$ rather than x^{-1}. It is customary to use additive notation only if $x + y = y + x$ for all $x, y \in G$.

In general, a group G (multiplicative again) is called *abelian* (or *commutative*) if $xy = yx$ for all $x, y \in G$.

We write $x^0 = 1, x^1 = x, x^2 = xx$, and in general $x^n = x^{n-1}x$ for $1 \leq n \in \mathbb{Z}$. Define $x^{-n} = (x^{-1})^n$, again for $1 \leq n \in \mathbb{Z}$. It is easy to verify by induction that the usual laws of exponents hold in any group, viz.,

$$x^m x^n = x^{m+n} \qquad \text{and} \qquad (x^m)^n = x^{mn}$$

for all $x \in G$, all $m, n \in \mathbb{Z}$. The additive analog of x^n is nx, so the additive analogs of the laws of exponents are $mx + nx = (m + n)x$ and $n(mx) = (mn)x$.

Exercise 1.1. Verify the laws of exponents for groups.

EXAMPLES

1. Let $G = \{1, -1\} \subseteq \mathbb{R}$, with multiplication as usual. Then G is a group.

2. Let $G = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, or $\mathbb{C}$, with the usual binary operation of addition. Then G is a group.

3. Let $G = \mathbb{Q}\backslash\{0\}$, the set of nonzero rational numbers, under multiplication. Then G is a group. Similarly this holds for $\mathbb{R}\backslash\{0\}$ and $\mathbb{C}\backslash\{0\}$, but *not* for $\mathbb{Z}\backslash\{0\}$. (Why?)

4. Let S be a nonempty set. A *permutation* of S (sometimes called a *bijection* of S) is a 1–1 function ϕ from S onto S. Let G be the set of all permutations of S. If $\phi, \theta \in G$, we define $\phi\theta$ to be their *composition* product, i.e., $\phi\theta(s) = \phi(\theta(s))$ for all $s \in S$. Composition is a binary operation on G (verify), and it is associative, for if $\phi, \theta, \sigma \in G$ and $s \in S$, then

$$(\phi(\theta\sigma))(s) = \phi(\theta\sigma(s)) = \phi[\theta(\sigma(s))],$$

and

$$((\phi\theta)\sigma)(s) = \phi\theta(\sigma(s)) = \phi[\theta(\sigma(s))].$$

G has an identity element, the permutation $1 = 1_S$ defined by $1(s) = s$, all $s \in S$, and each $\phi \in G$ has an inverse ϕ^{-1} defined by $\phi^{-1}(s_1) = s_2$ if and only if $\phi(s_2) = s_1$ (there are a few details to be verified). Thus G is a group; we write $G = \mathrm{Perm}(S)$. This example is of considerable importance and will be pursued much further.

5. As a special case of the preceding example take $S = \{1, 2, 3, \ldots, n\}$. The group G of all permutations of S is called the *symmetric group* on n letters and is denoted by $G = S_n$. If $\phi \in S_n$, it is convenient to display the function ϕ explicitly in the form

$$\phi = \begin{pmatrix} 1 & 2 & \cdots & n \\ \phi(1) & \phi(2) & \cdots & \phi(n) \end{pmatrix}.$$

For example, if $n = 3$, then $\phi = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right)$ is the permutation that maps 1 to 2, 2 to 3, and 3 to 1. The notation makes it quite simple to carry out explicit computations of the composition product. Suppose, for example, that $n = 3$ and $\phi = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right)$, $\theta = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{smallmatrix}\right)$. Note from the definition of $\phi\theta$ in Example 4 that θ acts first and ϕ second. Thus θ maps 1 to 3 and ϕ then maps 3 to 1, and so the composite $\phi\theta$ maps 1 to 1. Similarly, $\phi\theta$ maps 2 to 3 and maps 3 to 2. Thus

$$\phi\theta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Observe that

$$\theta\phi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \neq \phi\theta,$$

so S_3 is *not* an abelian group. It is easy to see that S_n is, likewise, not abelian for any $n > 3$, although S_1 and S_2 are abelian.

6. Let T be an equilateral triangle in the plane with center O. Let D_3 denote the set of *symmetries* of T, i.e., distance-preserving functions from the plane onto itself that carry T onto T (as a set of points). The elements of D_3 are called *congruences* of the triangle T in plane geometry. With composition as the binary operation, D_3 is a group. Let us list its elements explicitly. There is, of course, the identity function 1, with $1(x) = x$ for all x in the plane. There are two counterclockwise rotations, ϕ_1 and ϕ_2, about O as center through angles of 120° and 240°, respectively, and three mirror reflections θ_1, θ_2, θ_3 across the three lines passing through the vertices of T and through O (see Fig. 1).

It is edifying to cut a cardboard triangle, label the vertices, and determine composition products explicitly. The result is the "multiplication table" (Fig. 2) for D_3.

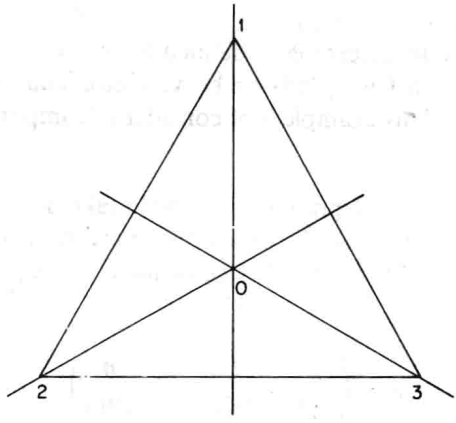

Figure 1

·	1	ϕ_1	ϕ_2	θ_1	θ_2	θ_3
1	1	ϕ_1	ϕ_2	θ_1	θ_2	θ_3
ϕ_1	ϕ_1	ϕ_2	1	θ_3	θ_1	θ_2
ϕ_2	ϕ_2	1	ϕ_1	θ_2	θ_3	θ_1
θ_1	θ_1	θ_2	θ_3	1	ϕ_1	ϕ_2
θ_2	θ_2	θ_3	θ_1	ϕ_2	1	ϕ_1
θ_3	θ_3	θ_1	θ_2	ϕ_1	ϕ_2	1

Figure 2

A routine inspection of the table shows that each element has an inverse, and also (if enough time is spent) that the operation is associative. Associativity is also clear from the fact that each element of D_3 is a permutation of the points of the plane. Thus D_3 is a group.

If we let $S = \{1, 2, 3\}$ be the set of vertices of T, then each element of D_3 gives rise to a permutation of S, i.e., to an element of the symmetric group S_3. For example, $\phi_1 \mapsto \left(\begin{smallmatrix}1&2&3\\2&3&1\end{smallmatrix}\right)$, $\theta_1 \mapsto \left(\begin{smallmatrix}1&2&3\\1&3&2\end{smallmatrix}\right)$, etc. The result is a 1–1 correspondence between the group D_3 of symmetries of T and the symmetric group S_3. It is instructive to label the elements of S_3 accordingly [e.g., $\alpha_1 = \left(\begin{smallmatrix}1&2&3\\2&3&1\end{smallmatrix}\right)$, $\beta_1 = \left(\begin{smallmatrix}1&2&3\\1&3&2\end{smallmatrix}\right)$, etc.], to write out the multiplication table for S_3 and to compare with the table above.

7. This time let T be a square in the plane, with center O, and let D_4 be its set (in fact group) of symmetries. There are four rotations (one of them the identity, through 0°) and four reflections (see Fig. 3). The multiplication table should be computed.

Again each element of D_4 gives rise to a permutation of the set $S = \{1, 2, 3, 4\}$ of vertices of T, i.e., to an element of S_4. For example, the rotation ϕ_1 through 90° counterclockwise about O gives the permutation $\alpha_1 = \left(\begin{smallmatrix}1&2&3&4\\2&3&4&1\end{smallmatrix}\right)$. Note in this case, however, that not all elements of S_4 occur. For example, $\left(\begin{smallmatrix}1&2&3&4\\2&1&3&4\end{smallmatrix}\right)$ is not the result of any symmetry of the square.

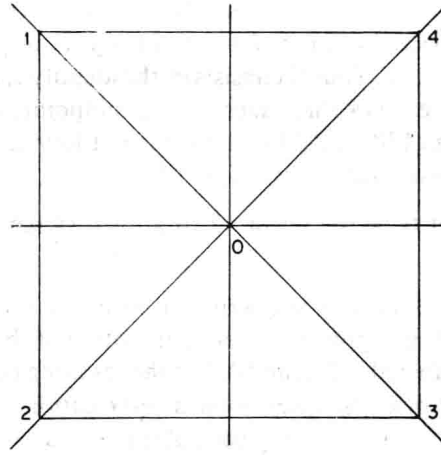

Figure 3

8. The quaternion group Q_2 consists of 8 matrices $\pm 1, \pm i, \pm j, \pm k$ under multiplication, where

$$i = \begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad j = \begin{bmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix}, \quad k = \begin{bmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

and 1 denotes the 4×4 identity matrix. It is easy to verify that $i^2 = j^2 = k^2 = -1$ and that $ij = k$. All other products can be determined from those. For example, since $ijk = k^2 = -1$ we have $i^2jk = -jk = -i$, and hence $jk = i$. The chief advantage of presenting Q_2 as a set of matrices is that the associative law is automatically satisfied.

9. Klein's 4-group K consists of four 2×2 matrices:

$$1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad a = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad b = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \text{and} \quad c = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Its multiplication table is Fig. 4.

·	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

Figure 4

10. Let T be a regular tetrahedron and let G be the set of all rotations of three-dimensional space that carry T to itself (as a set of points), i.e., all the *rotational symmetries* of T. Thus G consists of the identity 1, rotations through angles of 180° about each of three axes joining midpoints of opposite edges, and rotations through 120° and 240° about each of four axes joining vertices with centers of opposite faces. Thus $|G| = 12$.

Exercise 1.2. Let G be the set of 12 rotational symmetries of a regular tetrahedron.

(1) Verify that G is a group and write out its multiplication table.
(2) Each element of G gives rise to a permutation of the set of vertices of the tetrahedron, numbered 1, 2, 3, and 4. List the resulting permutations in S_4.
(3) Each element of G also gives rise to a permutation of the set of 6 edges of the tetrahedron. List the resulting permutations in S_6.

Exercise 1.3. Describe the groups of rotational symmetries of a cube (there are 24) and of a regular dodecahedron (there are 60). It will be helpful to have cardboard models.

Many more examples will appear as we continue. It will be convenient at this point to introduce some concepts, some terminology, and some elementary consequences of the definitions.

The cardinality $|G|$ of a group G is called its *order*. If G is not finite we usually say simply that G has *infinite order*. An easy counting argument shows that the symmetric group S_n has order $n!$.

A subset H of a group G is called a *subgroup* of G if the binary operation on G restricts to a binary operation on H under which H is itself a group. In that case the identity element of H must be the original identity 1 of G. (Why?) We write $H \leq G$ or $G \geq H$ to indicate that H is a subgroup of G. Referring to the additive groups $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ we have, for example, $\mathbb{Z} \leq \mathbb{Q}$, $\mathbb{Q} \leq \mathbb{R}$, and $\mathbb{Z} \leq \mathbb{R}$.

Proposition 1.4. If H is a nonempty subset of a group G, then $H \leq G$ if and only if $xy^{-1} \in H$ for all $x, y \in H$.

Proof. $\Rightarrow$: Obvious. $\Leftarrow$: Choose $x \in H$ and take $y = x$. Then $xy^{-1} = xx^{-1} = 1 \in H$. Next take $x = 1$ and any $y \in H$ to see that $1y^{-1} = y^{-1} \in H$. Thus $x(y^{-1})^{-1} = xy \in H$ whenever $x, y \in H$, so the multiplication on G restricts to a binary operation on H, which is associative since the original operation on G is associative. Thus H is a group and so $H \leq G$.

Exercise 1.4. If G is a *finite* group and $\varnothing \neq H \subseteq G$, show that H is a subgroup of G if and only if $xy \in H$ whenever $x \in H$, $y \in H$.

Proposition 1.5. If $\{H_\alpha\}$ is any collection of subgroups of a group G, then $\bigcap_\alpha H_\alpha \leq G$.